EXHIBIT A

herbalalchemist

MY ACCOUNT MY WISHLIST CHECKOUT LOG IN

CART: 0 ITEM(S) - $0.00

SUPPLEMENTS HERBALS & BOTANICALS WEIGHT MANAGEMENT SPORTS NUTRITION

Home > Privacy Policy

Effective on: (05/24/2015)
Herbal Alchemist is committed to your privacy. This notice serves to help you better understand what information Herbal Alchemist collects, how it uses that information, and with whom Herbal Alchemist may share a limited portion of that information with. The most recent version of Herbal Alchemist's privacy policy can be found on this page. If you have questions or concerns regarding this policy, you should contact Customer Support by email.

Herbal Alchemist knows that you value your personal information, and we protect your privacy as if it were our own. Herbal Alchemist's uses of your information is limited to the ways outlined in this notice, except as required by law and/or to comply with a judicial proceeding, court order, or legal process served on our website.

What kind of information about me does Herbal Alchemist collect?
Herbal Alchemist collects information about you in these ways:

Order information you give us: If you place an online order, our secure order form requests contact, billing, and financial information (such as your credit card numbers for purchases). Contact information from the order form (email address, name, billing and shipping address, and phone number) is used to send orders and information about our company to you.

Account information:
If you choose to create a Herbal Alchemist account, your login information is stored with any other information you associate with your account. Non-personal information we receive automatically: Like most websites, Herbal Alchemist utilizes cookies. Cookies are a mechanism to remember information about you when you navigate from one web page to another. Our website uses cookies to hold a user's unique session identifiers, allowing us to serve correct information back to the user. Such information includes your shopping cart items, or whether you are logged in. Our website cookies do not hold any personally identifiable information. Herbal Alchemist may use other similar technologies which allow us to collect non-personally identifiable information about your visit to help us better your experience. Mobile information: When you utilize our iPhone® or Android® phone apps, we may receive non-personally identifiable information, such as a unique identifier for your device letting us know what type of phone you are using.

How does Herbal Alchemist use this information?
Herbal Alchemist uses information collected in these ways:

Order processing and customer service:
After placing an online order, your contact information including your email address will be used to get in touch with you should we have questions regarding your order or should we need to notify you of the status of your order. Your credit card information is transmitted securely to our third part processing provider in compliance with Payment Card Industry standards. You will automatically be registered to receive our email newsletter, which you are able to opt out of at any time by accessing your user account, following the unsubscribe link found in the email newsletter.

Third-party service providers:
Herbal Alchemist works closely with other companies and individuals to facilitate transactions and better your experience. Examples of third-party service provider services include shipping orders, analyzing data, providing accurate search results and links, processing credit card payments, affiliate marketing, and newsletters. Any information that Herbal Alchemist shares with a third-party service provider is done so safely, securely, and under a contractual relationship with that provider to protect your data.

Promotional offers:
From time to time we or a service provider acting on our behalf may use your name, email address, and/or mailing address to send you an offer for a Herbal Alchemist product or service we believe to be of interest to you.

Other information you provide us:
Information you provide us for specific offers or services is only used for the limited purpose for which the information is being given. Examples of these offers or services include Refer-A-Friend, Email to a Friend, surveys, and sweepstakes.

What information can I access or modify?
If you are a registered customer, you may log into your account and view or modify the account information on file, including personally identifiable information, recent orders, payment settings, shopping lists, and Set & Save settings. In order to protect your personal information, only the last four numbers of any saved credit cards are viewable.

How does Herbal Alchemist secure my information?
Herbal Alchemist utilizes technologies including Transport Layer Security (TLS) and database encryption to ensure the privacy of your personal information. When you make an online purchase, our advanced security technology uses strong secure protocols to send your personal data to us, making it practically impossible for someone to intercept and extract that data. To further protect your information, we utilize state of the art back-end systems and restrict employee

MY CART

You have no items in your shopping cart.

COMPARE PRODUCTS

You have no items to compare.

NEWSLETTER

Sign Up for Our Newsletter:

SUBSCRIBE

access to your information. Anytime we share your information with a third party consistent with this Privacy Policy we utilize technological and contractual safeguards to keep your information safe.

While we are confident ordering online is safe and secure, if for any reason you cannot access the secure server or feel uncomfortable ordering online, please feel free to place your order with us by phone at 1-530-677-1200. As a general practice, it is important for you to protect against unauthorized access to your password and to your computer. If using a shared computer, be sure to log out of your account prior to leaving the computer.

Can I opt-out?
At any time you can adjust your communication preferences, including opting out of promotional mailings, from within your Herbal Alchemist account. You also have the right to disable your account. To do so, you may call or email Customer Service.

These statements have not been evaluated by the Food and Drug Administration.
Products mentioned on this site are not intended to diagnose, treat, cure or prevent any disease.
Actual product packaging and materials may contain more and different information than what is shown on our website.
We recommend that you do not rely solely on the information presented and that you always read labels, warnings, and directions before using or consuming any product.

EXHIBIT B

ISRG CPS v2.0

Internet Security Research Group (ISRG)

Certification Practice Statement

Version 2.0

Updated April 13, 2017

Approved by the ISRG Policy Management Authority

1. INTRODUCTION

1.1 Overview

This Certification Practice Statement ("CPS") document outlines the certification services practices for Internet Security Research Group ("ISRG") Public Key

Infrastructure ("ISRG PKI").

ISRG PKI services include, but are not limited to, issuing, managing, validating, revoking, and renewing Certificates in accordance with the requirements of the ISRG Certificate Policy (CP). It is recommended that readers familiarize themselves with the ISRG CP prior to reading this document.

ISRG PKI services are most commonly, but not necessarily exclusively, provided under the brand/trademark "Let's Encrypt".

The ISRG PKI conforms to the current version of the guidelines adopted by the Certification Authority/Browser Forum (“CAB Forum”) when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates (“Baseline Requirements”). CAB Forum documents can be found at https://www.cabforum.org. If there is any conflict between this CPS and a relevant CAB Forum requirement or guideline, then the CAB Forum requirement or guideline shall take precedence.

Other documents related to the behavior and control of the ISRG PKI, such as a Subscriber Agreement and Privacy Policy, can be found at https://letsencrypt.org/repository/.

Per IETF PKIX RFC 3647, this CPS is divided into nine components that cover security controls, practices, and procedures for certification services provided by the ISRG PKI.

The following Certification Authorities are covered under this CPS:

CA Type	Distinguished Name	Key Pair Type and Parameters	SHA-256 Key Fingerprint	Validity Period
	C=US, O=Internet		96:BC:EC:06:26:49:76:F3:	Not Before: Jun 4 11:04:38 2015

Root CA	Security Research Group, CN=ISRG Root X1	RSA, n has 4096 bits, e=65537	74:60:77:9A:CF:28:C5:A7:CF:E8:A3:C0:AA:E1:1A:8F:FC:EE:05:C0:BD:DF:08:C6	GMT, Not After: Jun 4 11:04:38 2035 GMT

1.2 Document name and identification

This is the ISRG Certification Practices Statement. This document was approved for publication by the ISRG Policy Management Authority, and is made available at https://letsencrypt.org/repository/.

The following revisions have been made:

Date	Changes	Version
May 5, 2015	Original.	1.0
September 9, 2015	Added/corrected a number of policy URIs, removed LDAP as mechanism for publishing certificate information, removed administrative contact requirement for DV-SSL subscribers, removed mention of web-based revocation option, removed description of customer service center, substantial changes to all of Section 9 regarding legal matters, other minor fixes/improvements.	1.1

September 22, 2015	Updated serial number description in Section 10.3.1, DV-SSL Certificate Profiles.	1.2
March 16, 2016	Update root CRL issuance periods, disallow issuance to '.mil' TLD, make NameConstraints extension optional for cross- certification profile, clarify optional NameConstraints contents, clarify that OSCP ResponderID is byname, clarify that OCSP nonce extension is not supported.	1.3
May 5, 2016	Reference CP v1.2 rather than CP v1.1. Add info about tlsFeature extension, serialNumber in Subject Distinguished Name field.	1.4
October 18, 2016	Do not require discontinuing use of a private key due to incorrect information in a certificate. Add information about issuance for Internationalized Domain Names. Add information about CA's CAA identifying domain. Do not require discontinuing use of a private key due to expiration or revocation of a certificate.	1.5
April 13, 2017	Complete rewrite of CPS.	2.0

1.3 PKI participants

1.3.1 Certification authorities

ISRG is a CA that provides services including, but not limited to, issuing, managing, validating, revoking, and renewing publicly-trusted Certificates. These services are performed in accordance with the requirements of the ISRG Certificate Policy (CP) and this CPS. These services are provided to the general public with exceptions as deemed appropriate by ISRG management or in accordance with relevant law.

ISRG PKI services are most commonly, but not necessarily exclusively, provided under the brand/trademark "Let's Encrypt".

1.3.2 Registration authorities

ISRG serves as its own RA. RA services are not performed by third parties.

1.3.3 Subscribers

See definition of "Subscriber" in Section 1.6.1 Definitions.

1.3.4 Relying parties

See definition of "Relying Party" in Section 1.6.1 Definitions.

Relying Parties must verify the validity of certificates via CRL or OCSP prior to relying on certificates. CRL and OCSP location information is provided within certificates.

1.3.5 Other participants

Other participants include CAs that cross-sign or issue subordinates to the ISRG PKI.

ISRG PKI vendors and service providers with access to confidential information or privileged systems are required to operate in compliance with the ISRG CP.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued by ISRG PKI can be used only to establish secure online communication between hosts (as identified by the FQDN provided in the Certificate) and clients using the TLS protocol.

1.4.2 Prohibited certificate uses

Certificates may not be used:

- For any purpose not explicitly defined in Section 1.4.1 of this document
- For any application requiring fail-safe performance such as a) the operation of nuclear power facilities b) air traffic control systems c) aircraft navigation systems d) weapons control systems e) any other system in which failure could lead to injury, death, or environmental damage.
- For software or hardware architectures that provide facilities for interference with encrypted communications, including but not limited to a) active eavesdropping (e.g., Man-in-the-middle attacks) b) traffic management of domain names or internet protocol (IP) addresses that the organization does not own or control. Note that these restrictions shall apply regardless of whether a relying party communicating through the software or hardware architecture has knowledge of its providing facilities for interference with encrypted communications.
- When prohibited by law.

Also, note that Certificates do not guarantee anything regarding reputation, honesty, or the current state of endpoint security. A Certificate only represents that the information contained in it was verified as reasonably correct when the Certificate was issued.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS document is maintained by the ISRG PMA.

1.5.2 Contact person

The ISRG PMA can be contacted at:

Policy Management Authority
Internet Security Research Group
1 Letterman Drive, Suite D4700
San Francisco, CA 94129

1.5.3 Person determining CPS suitability for the policy

The ISRG PMA is responsible for determining the suitability of this CPS. The ISRG PMA is informed by results and recommendations received from an independent auditor.

1.5.4 CPS approval procedures

The ISRG PMA approves any revisions to this CPS document after formal review.

1.6 Definitions and acronyms

1.6.1 Definitions

- ACME Protocol
    - A protocol used for validation, issuance, and management of certificates. The protocol is an open standard managed by the IETF.
- Applicant
    - An entity applying for a certificate.
- Baseline Requirements
    - A document published by the CAB Forum which outlines minimum requirements for publicly trusted Certificate Authorities.
- CAB Forum
    - Certificate Authority / Browser Forum, a group a CAs and browsers which come together to discuss technical and policy issues related to PKI systems. (https://cabforum.org/)

- Certificate Repository
    - A repository of information about ISRG certificates. It is located at: https://letsencrypt.org/certificates/
- Cross Certificate
    - A certificate that is used to establish a trust relationship between two Root CAs.
- Policy and Legal Repository
    - A repository of policy and legal documents related to the ISRG PKI. It is located at: https://letsencrypt.org/repository/
- Key Pair
    - A Private Key and its associated Public Key.
- Private Key
    - The key in a Key Pair that must be kept secret. Used to create digital signatures that can be verified by the corresponding Public Key or to decrypt messages encrypted by the corresponding Public Key.
- Public Key
    - The only key in a Key Pair that can safely be publicly disclosed. Used by Relying Parties to verify digital signatures from the corresponding private key or to encrypt messages that can only be decrypted by the corresponding private key.
- Relying Party
    - An entity that relies upon information contained within certificates issued by ISRG PKI services.
- Root CA
    - The top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.
- Secure PKI Facilities
    - Facilities designed to protect sensitive PKI infrastructure, including CA private keys.
- Subscriber
    - An entity that has agreed to a Subscriber Agreement and is using ISRG PKI services.

- Trusted Contributor
    - A contributor who performs in a Trusted Role. Trusted Contributors may be employees, contractors, or community members. Trusted Contributors must be properly trained and qualified, and have the proper legal obligations in place before performing in a Trusted Role.
- Trusted Role
    - A role which qualifies a person to access or modify ISRG PKI systems, infrastructure, and confidential information.

1.6.2 Acronyms

- ACME
    - Automated Certificate Management Environment
- BRs
    - Baseline Requirements
- CA
    - Certificate Authority
- CAA
    - Certificate Authority Authorization
- CP
    - Certificate Policy
- CPS
    - Certification Practice Statement
- DV
    - Domain Validation
- FQDN
    - Fully Qualified Domain Name
- HSM
    - Hardware Security Module
- IDN
    - Internationalized Domain Name
- IP
    - Internet Protocol

- ISRG
    - Internet Security Research Group
- PKI
    - Public Key Infrastructure
- PMA
    - Policy Management Authority
- RA
    - Registration Authority
- SAN
    - Subject Alternative Name
- TLD
    - Top Level Domain

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

ISRG CP, CPS, Privacy Policy, Subscriber Agreement, and WebTrust audit documents are made publicly available in the Policy and Legal Repository, which can be found at:

https://letsencrypt.org/repository/

2.2 Publication of certification information

Records of all ISRG root and intermediate certificates, including those that have been revoked, are available in the Certificate Repository:

https://letsencrypt.org/certificates/

ISRG certificates contain URLs to locations where certificate-related information is

published, including revocation information via OCSP and/or CRLs.

2.3 Time or frequency of publication

New or updated ISRG CP, CPS, Privacy Policy, Subscriber Agreement, and WebTrust audit documents are made publicly available as soon as possible. This typically means within seven days of receipt or approval.

New or updated ISRG root and intermediate certificates are made publicly available as soon as possible. This typically means within seven days of creation.

2.4 Access controls on repositories

Read only access to the Policy and Legal Repository and certificate information is unrestricted. Write access is protected by logical and physical controls.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Certificate distinguished names and subject alternative names are compliant with the CP.

3.1.2 Need for names to be meaningful

ISRG certificates include a "Subject" field which identifies the subject entity (i.e. organization or domain). The subject entity is identified using a distinguished name.

ISRG certificates include an "Issuer" field which identifies the issuing entity. The issuing entity is identified using a distinguished name.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers are not identified in DV certificates, which have subject fields identifying only domain names (not people or organizations). Relying parties should consider DV certificate subscribers to be anonymous.

3.1.4 Rules for interpreting various name forms

Distinguished names in certificates are to be interpreted using X.500 standards and ASN.1 syntax. RFC 2253 and RFC 2616 provide more information.

Certificates do not assert any specific relationship between subscribers and registrants of domain names contained in certificates.

Regarding Internationalized Domain Names, ISRG will have no objection so long as the domain is resolvable via DNS. It is the CA's position that homoglyph spoofing should be dealt with by registrars, and Web browsers should have sensible policies for when to display the punycode versions of names.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

ISRG reserves the right to make all decisions regarding Subscriber names in certificates. Entities requesting certificates will be required to demonstrate their right to use names (e.g. demonstrate control of a domain name), but trademark rights are not verified.

While ISRG will comply with U.S. law and associated legal orders, it is ISRG's

position that trademark enforcement responsibility for domain names should lie primarily with domain registrars and the legal system.

3.2 Initial identity validation

ISRG may elect not to issue any certificate at its sole discretion.

3.2.1 Method to prove possession of private key

Applicants are required to prove possession of the Private Key corresponding to the Public Key in a Certificate request, which can be done by signing the request with the Private Key.

3.2.2 Authentication of organization and domain identity

ISRG only issues Domain Validation (DV) certificates. Wildcard certificates are not supported. When a certificate request includes a list of FQDNs in a SAN list, all domains in the list are fully validated prior to issuance.

Validation for DV certificates involves demonstrating proper control over a domain. ISRG validates domain control primarily in an automated fashion via the ACME protocol. In exceptional cases control may be validated using methods similar to those employed by ACME, but performed manually.

There are three methods used for demonstrating domain control:

1. Agreed-Upon Change to Website: Confirming the Applicant's control over the requested FQDN by confirming the presence of agreed-upon content contained in a file or on a web page under the "/.well-known/acme-challenge/" directory on the requested FQDN that is accessible to the CA via HTTP over port 80, following redirects. (BR Section 3.2.2.4.6)

2. DNS Change: Confirming the Applicant's control over the requested FQDN

by confirming the presence of a random value (with at least 128 bits entropy) in a DNS TXT or CAA record for the requested FQDN prefixed with the label '_acme-challenge'. (BR Section 3.2.2.4.7)

3. TLS Using a Random Number: Confirming the Applicant's control over the requested FQDN by confirming the presence of a random value (with at least 128 bits entropy) within a Certificate on the requested FQDN which is accessible to the CA via TLS over port 443. (BR Section 3.2.2.4.10)

3.2.3 Authentication of individual identity

ISRG does not issue certificates to individuals, and thus does not authenticate individual identities.

3.2.4 Non-verified subscriber information

Non-verified Applicant information is not included in ISRG certificates.

3.2.5 Validation of authority

ISRG does not issue certificates to organizations, and thus does not validate any natural person's authority to request certificates on behalf of organizations.

Organizations have the option to specify CA issuance authority via CAA records, which ISRG respects.

3.2.6 Criteria for interoperation

ISRG discloses Cross Certificates in its Certificate Repository:

https://letsencrypt.org/certificates/

3.3 Identification and authentication for re-key requests

ISRG does not support re-key requests. Subscribers must request new certificates.

3.3.1 Identification and authentication for routine re-key

See Section 3.3 text.

3.3.2 Identification and authentication for re-key after revocation

See Section 3.3 text.

3.4 Identification and authentication for revocation request

Identification and authentication for revocation requests is performed by ISRG in compliance with Section 4.9 of this document.

Identification and authentication is not required when revocation is being requested by ISRG.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Anyone may submit an application for a certificate via the ACME protocol. Issuance

will depend on proper validation and compliance with ISRG policies.

4.1.2 Enrollment process and responsibilities

The enrollment process involves the following steps, in no particular order:

- Generating a key pair using secure methods
- Submitting a request for a certificate containing all necessary information, including the public key
- Agreeing to the relevant Subscriber Agreement

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

ISRG performs all identification and authentication functions in accordance with the ISRG CP. This includes validation per CPS Section 3.2.2.

ISRG checks for relevant CAA records prior to issuing certificates. The CA acts in accordance with CAA records if present. The CA's CAA identifying domain is 'letsencrypt.org'.

4.2.2 Approval or rejection of certificate applications

Approval requires successful completion of validation per Section 3.2.2 as well as compliance with all CA policies.

Certificates containing a new gTLD under consideration by ICANN will not be issued. The CA Server will periodically be updated with the latest version of the Public Suffix List and will consult the ICANN domains section for every requested DNS identifier. CA server will not validate or issue for DNS identifiers that do not have a Public Suffix in the ICANN domains section. The Public Suffix List is updated when new gTLDs are added, and never includes new gTLDs before they are

resolvable.

ISRG maintains a list of high-risk domains and blocks issuance of certificates for those domains. Requests for removal from the high-risk domains list will be considered, but will likely require further documentation confirming control of the domain from the Applicant, or other proof as deemed necessary by ISRG management.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificates issued by the Root CA require an individual authorized by ISRG to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

The source of a certificate request is confirmed before issuance. CA processes are protected from unauthorized modification during certificate issuance. Issued certificates are stored in a database and then made available to the Subscriber.

4.3.2 Notification to subscriber by the CA of issuance of certificate

End-entity certificates are made available to Subscribers via the ACME protocol as soon after issuance as reasonably possible. Typically this happens within a few seconds.

All end-entity certificates are logged to Certificate Transparency servers as soon as reasonably possible. Typically this happens within a few seconds.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

See ISRG CP Section 4.4.1.

4.4.2 Publication of the certificate by the CA

All root and intermediate certificates are made available publicly via the Certificate Repository.

All end-entity certificates are made available to Subscribers via the ACME protocol.

All end-entity certificates are logged to Certificate Transparency servers.

4.4.3 Notification of certificate issuance by the CA to other entities

See Section 4.4.2.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Subscribers are obligated to generate Key Pairs using reasonably trustworthy systems.

Subscribers are obligated to take reasonable measures to protect their Private Keys from unauthorized use or disclosure (which constitutes compromise). Subscribers must discontinue use of any Private Keys that are known or suspected to have been compromised.

Certificates must be used in accordance with their intended purpose, which is

outlined in this CPS and the associated CP. Subscribers must cease use of certificates being used outside of their intended purpose.

4.5.2 Relying party public key and certificate usage

Relying Parties must fully evaluate the context in which they are relying on certificates and the information contained in them, and decide to what extent the risk of reliance is acceptable. If the risk of relying on a certificate is determined to be unacceptable, then Relying Parties should not use the certificate or should obtain additional assurances before using the certificate.

ISRG does not warrant that any software used by Relying Parties to evaluate or otherwise handle certificates does so properly.

Relying Parties ignoring certificate expiration, revocation data provided via OCSP or CRL, or other pertinent information do so at their own risk.

4.6 Certificate renewal

Certificate renewal requests are treated as applications for new certificates.

4.7 Certificate re-key

Certificate re-key requests are treated as applications for new certificates.

4.8 Certificate modification

Certificate modification requests are treated as applications for new certificates.

4.9 Certificate revocation and suspension

Certificate revocation permanently ends the certificate's operational period prior to its stated validity period.

4.9.1 Circumstances for revocation

ISRG will follow the ISRG CP and revoke a certificate in accordance with Section 4.9.1.1 and Section 4.9.1.2 of the ISRG CP.

ISRG maintains a continuous (24x7x365) ability to accept and respond to revocation requests and related inquiries.

4.9.2 Who can request revocation

Anyone can revoke any certificate via the ACME API if they can sign the revocation request with the private key associated with the certificate. No other information is required in such cases. A number of ACME clients support this functionality.

Anyone can revoke any certificate via the ACME API if they can demonstrate control over all domains covered by the certificate. No other information is required in such cases. A number of ACME clients support this functionality.

Subscribers can revoke certificates belonging to their accounts via the ACME API if they can sign the revocation request with the associated account private key. No other information is required in such cases. A number of ACME clients support this.

Certificates may be administratively revoked by ISRG if it is determined that the Subscriber has failed to meet obligations under the CP, this CPS, the relevant Subscriber Agreement, or any other applicable agreement, regulation, or law. Certificates may also be administratively revoked at the discretion of ISRG management.

4.9.3 Procedure for revocation request

Revocation requests may be made at any time via the ACME API.

All other requests for revocation must be made by emailing cert-prob-reports@letsencrypt.org. ISRG will respond to such requests within 24 hours, though an investigation into the legitimacy of the request may take longer.

An investigation into whether revocation or other appropriate action is warranted will be based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint; and
4. Relevant legislation.

4.9.4 Revocation request grace period

There is no grace period for a revocation request. A revocation request must be made as soon as circumstances requiring revocation are confirmed.

4.9.5 Time within which CA must process the revocation request

Investigation into a revocation request will begin within 24 hours of receiving the request.

Once a decision has been made to revoke a certificate, revocation will be carried out within 24 hours.

4.9.6 Revocation checking requirement for relying parties

Relying Parties who cannot or choose not to check revocation status, but decide to rely on a certificate anyway, do so at their own risk.

See Section 4.5.2.

4.9.7 CRL issuance frequency (if applicable)

ISRG will issue updated CRLs for intermediate certificates with a frequency greater

than or equal to that required by the ISRG CP.

ISRG does not issue CRLs for end-entity certificates.

4.9.8 Maximum latency for CRLs (if applicable)

When a CRL is requested by a Relying Party the time to receive a response will be less than ten seconds under normal operating conditions.

4.9.9 On-line revocation/status checking availability

Revocation information for all certificates is made available via OCSP. OCSP responses are available at all times (24x7x365) if possible.

4.9.10 On-line revocation checking requirements

See Section 4.9.6.

4.9.11 Other forms of revocation advertisements available

ISRG allows for OCSP stapling.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

ISRG does not suspend certificates.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

CRL entries for intermediate certificates will remain in place until the certificates expire. ISRG does not provide CRLs for end-entity certificates.

OCSP responses will be made available for all unexpired certificates.

4.10.2 Service availability

All certificate status services are made available at all times (24x7x365) if possible.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

A Subscriber's subscription ends once all of Subscriber's ISRG certificates have expired or been revoked.

Prior to the end of subscription, ISRG will send the Subscriber notice of pending Certificate expiration, in the form of a renewal notification, when 20% of the certificate’s lifetime remains, if a contact email address was provided.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

5.1.1 Site location and construction

ISRG Secure PKI Facilities are located in the United States, as are all copies of CA root and intermediate private keys.

ISRG maintains at least two Secure PKI Facilities at all times for the sake of redundancy.

Secure PKI Facilities are constructed so as to prevent unauthorized entry or interference.

Secure PKI Facilities are monitored at all times (24x7x365) so as to prevent unauthorized entry or interference.

5.1.2 Physical access

Physical access to ISRG Secure PKI Facilities is restricted to authorized ISRG employees, vendors, and contractors, for whom access is required in order to execute their jobs. Access restrictions are strongly enforced via multi-factor authentication mechanisms.

5.1.3 Power and air conditioning

Redundant power sources are readily available at each Secure PKI Facility, and are designed to meet ISRG's operating requirements.

Air conditioning systems at each Secure PKI Facility are designed to meet ISRG's operating requirements.

5.1.4 Water exposures

ISRG Secure PKI Facilities are designed to protect ISRG infrastructure from water exposure/damage.

5.1.5 Fire prevention and protection

ISRG Secure PKI Facilities are designed to prevent fire and provide suppression if necessary.

5.1.6 Media storage

ISRG Secure PKI Facilities are designed to prevent accidental damage or unauthorized access to media.

5.1.7 Waste disposal

ISRG prohibits any media that contains or has contained sensitive data from leaving organizational control in such a state that it may still be operational, or contain

recoverable data. Such media may include printed documents or digital storage devices. When media that has contained sensitive information reaches its end of life, the media is physically destroyed such that recovery is reasonably believed to be impossible.

5.1.8 Off-site backup

ISRG maintains multiple backups of private keys at multiple Secure PKI Facilities. All backups are stored on devices meeting FIPS 140 Level 3 criteria.

5.2 Procedural controls

5.2.1 Trusted roles

All persons, employees or otherwise, with the ability to materially impact the operation of ISRG PKI systems and services, or the ability to view CA confidential information, must do so while designated as serving in a Trusted Role.

Trusted Roles include, but are not limited to:

- Management
    - May view confidential information but may not directly impact CA operations. Strong decision-making authority.
- Security Officers
    - May view confidential information but may not directly impact CA operations. Strong decision-making authority.
- Systems Administrators
    - May view confidential information and directly impact CA operations. Decision-making authority is limited.
- Engineering Liaisons
    - May view confidential information but may not directly impact CA operations. No decision-making authority.

Each Trusted Role requires an appropriate level of training and legal obligation.

5.2.2 Number of persons required per task

A number of tasks, such as key generation and entering areas physically containing operating ISRG PKI systems, require at least two people in Trusted Roles to be present.

5.2.3 Identification and authentication for each role

Anyone performing work in a Trusted Role must identify and authenticate themselves before accessing ISRG PKI systems or confidential information.

5.2.4 Roles requiring separation of duties

Nobody with the ability to deploy software to ISRG PKI systems (e.g. Systems Administrators) may have the ability to commit code to core CA software. The reverse is also true.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

ISRG management is responsible for making sure that Trusted Contributors are trustworthy and competent, which includes having proper qualifications and experience.

ISRG management ensures this with appropriate interviewing practices, training, background checks, and regular monitoring and review of Trusted Contributor job performance.

5.3.2 Background check procedures

Trusted Contributors must undergo a background check prior to performing in a

trusted role. ISRG management will review the results of background checks for problematic issues prior to approving performance of a trusted role.

Background checks include, but are not limited to, criminal background and employment history.

5.3.3 Training requirements

Trusted Contributors must be trained on topics relevant to the role in which they will perform.

Training programs are developed for each role by ISRG management and Security Officers.

5.3.4 Retraining frequency and requirements

Training is repeated for each Trusted Contributor on an annual basis and re-covers all topics relevant to their trusted role.

Training is also offered whenever changes in the industry or operations require it in order for contributors to competently perform in their trusted roles.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Action will be taken to safeguard ISRG and its subscribers whenever ISRG Trusted Contributors, whether through negligence or malicious intent, fail to comply with ISRG policies including this CPS.

Actions taken in response to non-compliance may include termination, removal from trusted roles, or reporting to legal authorities.

Once management becomes aware of non-compliance the Trusted Contributor(s) in

question will be removed from trusted roles until a review of their actions is complete.

5.3.7 Independent contractor requirements

Independent contractors who are assigned to perform Trusted Roles are subject to the duties and requirements specified for such roles in this CPS and the accompanying CP. This includes those described in Section 5.3. Potential sanctions for unauthorized activities by independent contractors are described in Section 5.3.6.

5.3.8 Documentation supplied to personnel

Trusted Contributors are provided with all documentation necessary to perform their duties. This always includes, at a minimum, a copy of the ISRG CP, CPS, and Information Security Policy.

5.4 Audit logging procedures

5.4.1 Types of events recorded

Audit logs are generated for all events related to CA security (physical and logical) and certificate issuance. Logs are automatically generated whenever possible. When it is necessary to manually log information, logs are kept on paper with written confirmation from a witness and securely stored. All audit logs, electronic or otherwise, shall be retained and made available to compliance auditors upon request.

At a minimum, each audit record includes:

- Date and time of entry;
- Identity of the person (or machine) making the entry; and
- Description of the entry.

5.4.2 Frequency of processing log

No stipulation.

5.4.3 Retention period for audit log

Audit logs are retained for at least seven years and will be made available to compliance auditors upon request.

5.4.4 Protection of audit log

Audit logs, whether in production or archived, are protected using both physical and logical access controls.

5.4.5 Audit log backup procedures

ISRG makes regular backup copies of audit logs. Audit log backup copies are sent for secure offsite storage at least once per month.

5.4.6 Audit collection system (internal vs. external)

Audit data is automatically generated and reported/recorded by operating systems, CA software applications, and network devices. Systems are in place to ensure proper reporting and recording of audit data, and the failure of such systems may lead to suspension of CA services until proper audit log reporting is restored.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Audit logs are monitored by Trusted Contributors, including operations and engineering staff. Anomalies indicating attempted breaches of CA security are

reported and investigated.

Automated internal and external vulnerability scans occur at least every two weeks, though more typically every week.

Extensive vulnerability assessments for ISRG infrastructure and primary CA application code are conducted at least annually by qualified third parties.

ISRG Security Officers perform a risk assessment at least annually. This risk assessment:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.5 Records archival

5.5.1 Types of records archived

ISRG archives all audit logs, the contents of which are described in Section 5.4.1. ISRG may also archive any other information deemed critical to understanding the historical performance of the CA's duties.

5.5.2 Retention period for archive

ISRG retains all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any

Certificate based on that documentation ceases to be valid.

5.5.3 Protection of archive

Archives are protected from unauthorized modification or destruction by strong security and environmental controls at primary and offsite storage facilities.

5.5.4 Archive backup procedures

Archives are backed up at primary CA facilities as well as at secure off-site facilities.

5.5.5 Requirements for time-stamping of records

Records are time-stamped as they are created.

Machine-created records use system time, which is synchronized automatically with third-party time sources. Machines without network access have the time set manually.

Manual records use a manually entered date and time, complete with time zone in use.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

When a CA certificate is nearing expiration, a key changeover procedure is used to

transition to a new CA certificate. The following steps constitute a key changeover procedure:

1. Some time prior to CA certificate expiration, the private key associated with the expiring certificate is no longer used to sign new certificates. It is only used to sign CRLs and OCSP responses.
2. A new key pair is generated and a new CA certificate is created containing the new key pair's public key. This new key pair is used to sign new certificates.
3. If necessary or desired, the old private key associated with the expiring certificate may be used to cross-sign the new certificate.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

ISRG has created and maintains incident response procedures for a range of potential compromise and disaster situations. Such situations include, but are not limited to, natural disasters, security incidents, and equipment failure. Incident response plans are reviewed, potentially updated, and tested on at least an annual basis.

5.7.2 Computing resources, software, and/or data are corrupted

In the event that computing resources, software, and/or data are corrupted or otherwise damaged, ISRG will assess the situation, including its impact on CA integrity and security, and take appropriate action. CA operations may be suspended until mitigation is complete. Subscribers may be notified if corruption or damage has a material impact on the service provided to them.

5.7.3 Entity private key compromise procedures

In the event that a CA Private Key is compromised, or suspected to be compromised, ISRG will immediately launch a thorough investigation. Forensic evidence will be collected and secured as quickly as possible. If it cannot be determined with a high degree of certainty that the private key in question was not compromised, then the following steps may be taken in whatever order is deemed most appropriate by ISRG Security Officers:

- Certificates relying on the private key in question will be revoked.
- ISRG will notify root programs relying on the integrity of the key in question.
- ISRG will notify Subscribers relying on the integrity of the key in question.

5.7.4 Business continuity capabilities after a disaster

ISRG maintains multiple geographically diverse facilities, each of which is capable of operating ISRG CA systems independently. In the event that a disaster entirely disables one facility, ISRG CA operations will fail over to another facility.

5.8 CA or RA termination

In the event that ISRG CA services are to be terminated:

- All affected parties, including root programs and Subscribers, will be provided with notice as far in advance as reasonably possible.
- A termination plan will be created and review by the ISRG PMA.

If a suitable successor entity exists, the following steps will be taken:

- CA Private Keys, records, logs, and other critical documentation will be transferred to the successor organization in a secure and compliant manner.
- Arrangements will be made for compliant continuation of CA responsibilities.

If a suitable successor entity does not exist, the following steps will be taken:

- All certificates issued will be revoked and final CRLs will be published.
- CA Private Keys will be destroyed.
- CA records, logs, and other critical documentation will be transferred to a third party or government entity with appropriate legal controls in place to protect information while allowing its use in compliance with relevant policies and the law.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

CA private keys are generated by HSMs meeting the requirements of Section 6.2.1. This occurs during a ceremony meeting the requirements of this CPS and the accompanying CP.

Subscriber key pairs are generated and managed by Subscribers. Generation and management of Subscriber key pairs must be done in compliance with the terms of the CA Subscriber Agreement and ISRG CPS Section 9.6.3.

6.1.2 Private key delivery to subscriber

ISRG never generates or has access to Subscriber Private Keys.

6.1.3 Public key delivery to certificate issuer

Subscriber Public Keys are communicated to ISRG electronically via the ACME

protocol.

6.1.4 CA public key delivery to relying parties

ISRG Public Keys are provided to Relying Parties as part of browser, operating system, or other software trusted root certificate lists.

ISRG Public Keys are also available on ISRG websites such as letsencrypt.org.

6.1.5 Key sizes

ISRG CA root Private Keys are RSA keys at least 4096 bits in length.

ISRG CA intermediate Private Keys are RSA keys at least 2048 bits in length.

6.1.6 Public key parameters generation and quality checking

ISRG uses HSMs conforming to FIPS 186-4, capable of providing random number generation and on-board creation of at least 2048-bit RSA keys.

Per Section 5.3.3, NIST SP 800-89, the CA ensures that the public exponent of the RSA Keys for a DV-SSL Certificates is in the range between $2^{16}+1$ and $2^{256}-1$. The moduli are an odd number, not the power of a prime, and have no factors smaller than 752.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

See Section 7, Certificate Profiles.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

ISRG uses HSMs meeting FIPS 140-2 Level 3 (or higher) requirements.

6.2.2 Private key (n out of m) multi-person control

ISRG has put into place security mechanisms which require multiple people performing in Trusted Roles in order to access CA Private Keys, both physically and logically. This is true for all copies of Private Keys, in production or backups, on-site or off-site.

6.2.3 Private key escrow

ISRG does not escrow CA Private Keys and does not provide such a service for Subscribers.

6.2.4 Private key backup

Critical ISRG Private Keys are backed up both on-site and off-site, in multiple geographic locations, under multi-person control.

6.2.5 Private key archival

ISRG does not archive private keys.

6.2.6 Private key transfer into or from a cryptographic module

ISRG CA Private Keys are generated inside HSMs and are only transferred between HSMs for redundancy or backup purposes. When transferred, keys are encrypted prior to leaving HSMs and unwrapped only inside destination HSMs. Keys never exist in plain text form outside of HSMs.

6.2.7 Private key storage on cryptographic module

ISRG CA Private Keys are stored on HSMs meeting the requirements stated in Section 6.2.1.

6.2.8 Method of activating private key

ISRG CA Private Keys are always stored on HSMs and activated using the mechanisms provided by the HSM manufacturer. Activation data and devices are protected.

6.2.9 Method of deactivating private key

ISRG CA Private Keys are always stored on HSMs and deactivated using the mechanisms provided by the HSM manufacturer.

6.2.10 Method of destroying private key

ISRG CA Private Keys are destroyed by Trusted Contributors using a FIPS 140-2 (or higher) validated zeroize method provided by the HSMs storing the keys. Physical destruction of the HSM is not required.

Subscribers are obligated to securely destroy private keys when they should no longer be used, in most cases by securely deleting all copies of private key files from storage media.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other aspects of key pair management

6.3.1 Public key archival

See Section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

The lifetimes of ISRG Root CA certificates are specified in Section 1.1. Corresponding key pairs have the same lifetimes.

End-entity certificates issued by ISRG to Subscribers shall have a validity period less than 100 days. Subscriber key pairs may be re-used indefinitely provided that there is no suspicion or confirmation of Private Key compromise.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data used to activate CA Private Keys is generated during a key ceremony. Activation data is transferred to the person who will use it, or place it will be stored, in a secure fashion.

6.4.2 Activation data protection

Activation data is protected from unauthorized disclosure via a combination of physical and logical means.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical

requirements

ISRG CA infrastructure and systems are appropriately secured in order to protect CA software and data from unauthorized access or modification. Access to systems is secured via multi-factor authentication whenever possible. Security updates are applied in a timely fashion. Vulnerability scans are run regularly.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

ISRG has developed policies and procedures to effectively manage the acquisition and development of its CA systems.

ISRG CA hardware and software is dedicated solely to performing CA functions.

Vendor selection includes an evaluation of reputation in the market, ability to deliver a quality product, vulnerability history, and the likelihood of remaining viable in the future. Purchases are made in such a way that as little information about the future use of products as possible is disclosed. Physical product deliveries are received by Trusted Contributors and inspected for evidence of tampering. HSMs are shipped in tamper-evident packaging and tamper bag serial numbers are confirmed with the vendor upon reception.

ISRG maintains a CA testing environment separate from the production environment. The testing environment matches the production environment as closely as reasonably possible but does not have access to CA Private Keys used in trusted certificates. The purpose of this testing platform is to allow extensive but safe testing of software and systems that are or will be deployed to the CA production environment.

ISRG has developed and maintains appropriate change control policies and procedures to be followed any time CA systems are modified. Changes to ISRG CA systems require review by qualified Trusted Personnel who are different from the person requesting the change. Change requests are documented, as are any subsequent required reviews or approvals.

When ISRG develops software to be used in CA operations, software development policies are put into place and methodologies are followed in order to ensure software quality and integrity. This always includes a requirement for peer review of code changes. Unit testing is strongly encouraged. Code commit privileges are granted only to qualified and trusted contributors. Nobody with the ability to deploy software to ISRG PKI systems (e.g. Systems Administrators) may have the ability to commit code to core CA software. The reverse is also true.

6.6.2 Security management controls

ISRG has mechanisms in place to control and monitor security-related configuration of CA systems. Equipment and software is installed and configured using a documented change control process. Software integrity is verified upon deployment using checksums.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

ISRG implements reasonable network security safeguards and controls to prevent unauthorized access to CA systems and infrastructure. ISRG's network is multi-tiered and utilizes the principle of defense in depth.

Firewalls and other critical CA systems are configured based on a necessary-traffic-only whitelisting policy whenever possible.

ISRG root CA Private Keys are stored offline in a secure manner.

6.8 Time-stamping

See Section 5.5.5.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

All fields are as specified in RFC5280, including fields and extensions not specifically mentioned. Extensions are not marked critical unless specifically described here as critical.

Root CA Certificate

Field or extension	Value
Serial Number	Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	C=US, O=Internet Security Research Group, CN=ISRG Root X<n> where n is an integer representing the instance of the Root CA Certificate. For example, ISRG Root X1, ISRG Root X2, etc.
Subject Distinguished Name	Same as Issuer DN

Validity Period	Up to 25 years
Basic Constraints	Critical. cA=True, pathLength constraint absent
Key Usage	Critical. keyCertSign, cRLSign

Intermediate CA Certificate

Field or extension	Value
Serial Number	Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	Derived from Issuer certificate
Subject Distinguished Name	C=US, O=Let's Encrypt, CN=Let's Encrypt Authority X<n> where n is an integer representing the instance of the Subordinate CA Certificate
Validity Period	Up to 8 years
Basic Constraints	Critical. cA=True, pathLength constraint 0
Key Usage	Critical. keyCertSign, cRLSign, digitalSignature
Extended Key Usage	TLS Server Authentication, TLS Client Authentication
Certificate Policies	CAB Forum Domain Validated (2.23.140.1.2.1) ISRG Domain Validated (1.3.6.1.4.1.44947.1.1.1) Policy Qualifier Id=CPS Qualifier: Pointer to this CPS

Authority Information Access	Contains CA Issuers URL and OCSP URL. URLs vary based on Issuer.
CRL Distribution Points	Contains a CRL URL. URL varies based on Issuer.

DV-SSL End Entity Certificate

Field or extension	Value
Serial Number	Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	Derived from Issuer certificate
Subject Distinguished Name	CN=one of the values from the Subject Alternative Name extension
Validity Period	90 days
Basic Constraints	Critical. cA=False
Key Usage	Critical. digitalSignature, keyEncipherment
Extended Key Usage	TLS Server Authentication, TLS Client Authentication
Certificate Policies	CAB Forum Domain Validated (2.23.140.1.2.1) ISRG Domain Validated (1.3.6.1.4.1.44947.1.1.1) CPS Qualifier: Pointer to this CPS User Notice Qualifier: As specified in ISRG CPS section 7.1.8

Authority Information Access	Contains CA Issuers URL and OCSP URL. URLs vary based on Issuer.
Subject Public Key	RSA with modulus between 2048 and 4096, inclusive; or namedCurve P-256; or namedCurve P-384
Subject Alternative Name	A sequence of 1 to 100 dNSNames
TLS Feature	Contains status_request if requested by the subscriber in the CSR

Root OCSP Signing Certificate

Signed by a Root CA Certificate, these Certificates sign OCSP responses for Intermediate CA Certificates.

Field or extension	Value
Serial Number	Must be unique, with 64 bits of output from a CSPRNG
Issuer Distinguished Name	C=US, O=Internet Security Research Group, CN=ISRG Root X<n>
Subject Distinguished Name	C=US, O=Internet Security Research Group, CN=ISRG Root OCSP X<n>
Validity Period	5 years
Basic Constraints	Critical. cA=False
Key Usage	Critical. digitalSignature
Extended Key	Critical.

Usage	OCSPSigning
No Check	Present

7.1.1 Version number(s)

All certificates use X.509 version 3.

7.1.2 Certificate extensions

See section 7.1.

7.1.3 Algorithm object identifiers

Name	Object identifier
sha256WithRSAEncryption	1.2.840.113549.1.1.11

7.1.4 Name forms

See ISRG Certificate Policy.

7.1.5 Name constraints

By policy, ISRG will not issue Certificates for IP addresses or the .mil TLD. These restrictions are not enforced by a NameConstraints extension.

7.1.6 Certificate policy object identifier

See section 7.1.

7.1.7 Usage of Policy Constraints extension

Not applicable.

7.1.8 Policy qualifiers syntax and semantics

See section 7.1.

7.1.9 Processing semantics for the critical Certificate Policies extension

Not applicable.

7.2 CRL profile

Field or Extension	Value
Version	V2
Signature Algorithm	sha256WithRSAEncryption
ThisUpdate	The date and time when the Certificate revocation list was issued.
NextUpdate	ThisUpdate + 30 days
RevokedCertificates	Contains: userCertificate, revocationDate, reasonCode
CRLnumber	The serial number of this CRL in an incrementally increasing sequence of CRLs.

7.2.1 Version number(s)

See section 7.2.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

ISRG OCSP responders implement the RFC 5019 profile of RFC 6960.

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

WebTrust compliance audits are intended to ensure a CA's compliance with its CP and CPS and relevant WebTrust audit criteria.

8.1 Frequency or circumstances of assessment

WebTrust compliance audit periods cover no more than one year and are scheduled by ISRG annually, every year with no gaps.

See Section 8.7 for information about the frequency of self-audits.

8.2 Identity/qualifications of assessor

ISRG's WebTrust compliance audits are performed by a qualified auditor. A qualified auditor means a natural person, legal entity, or group of natural persons or legal entities that collectively possess the following qualifications and skills:

1. Independence from the subject of the audit (which is ISRG);
2. The ability to conduct an audit that addresses the relevant criteria
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's relationship to assessed entity

ISRG's WebTrust auditors shall have no financial interest in, or other type of relationship with, ISRG, which might cause the auditors to have a bias for or against ISRG.

8.4 Topics covered by assessment

Compliance audits cover ISRG's compliance with the ISRG CP and this CPS, as well as the following WebTrust principles and criteria:

- Principles and Criteria for Certification Authorities
- WebTrust Principles and Criteria for Certification Authorities – SSL Baseline with Network Security

8.5 Actions taken as a result of deficiency

Noncompliance with relevant requirements will be documented by auditors (internal or external), the ISRG PMA will be informed, and the ISRG PMA will ensure that steps are taken to address the issues as quickly as reasonably possible.

8.6 Communication of results

Audit results are reported to the ISRG PMA and any other entity entitled to the results by law, regulation, or agreement. This includes a number of Web user agent (i.e. browser) root programs.

ISRG is not required to publicly disclose any audit finding that does not impact the overall audit opinion.

8.7 Self-Audits

ISRG performs a quarterly internal audit of at least 3% of issuance since the last WebTrust audit period. The sample is randomly selected. Results are saved and provided to auditors upon request.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

ISRG does not charge any fees for certificate issuance or renewal.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

ISRG does not charge any fees for certificate revocation or for checking the validity status of an issued certificate using a CRL or OSCP.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

ISRG collects no fees, and so provides no refunds.

9.2 Financial responsibility

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

ISRG employees, agents, and contractors are responsible for protecting confidential information and are bound by ISRG's policies with respect to the treatment of confidential information or are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4 Privacy of personal information

9.4.1 Privacy plan

ISRG follows the privacy policy posted on its website (https://letsencrypt.org/repository/) when handling personal information.

9.4.2 Information treated as private

The privacy policy posted on ISRG's website (https://letsencrypt.org/repository/) identifies information that ISRG treats as private.

9.4.3 Information not deemed private

The privacy policy posted on ISRG's website (https://letsencrypt.org/repository/) identifies information that ISRG does not treat as private.

9.4.4 Responsibility to protect private information

ISRG employees and contractors are subject to policies or contractual obligations requiring them to comply with ISRG's privacy policy (https://letsencrypt.org/repository/) or contractual obligations at least as protective of private information as ISRG's privacy policy.

9.4.5 Notice and consent to use private information

ISRG follows the privacy policy posted on its website (https://letsencrypt.org/repository/) when using personal information.

9.4.6 Disclosure pursuant to judicial or administrative process

ISRG may disclose personal information if compelled to do so by court order or other compulsory legal process, provided that ISRG will oppose such disclosure with all legal and technical tools reasonably available to ISRG.

9.4.7 Other information disclosure circumstances

ISRG may disclose personal information under other circumstances that are described in the privacy policy posted on its website (https://letsencrypt.org/repository/).

9.5 Intellectual property rights

ISRG and/or its business partners own the intellectual property rights in ISRG's

services, including the certificates, trademarks used in providing the services, and this CPS. Certificate and revocation information are the property of ISRG. ISRG grants permission to reproduce and distribute certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys remain the property of the Subscribers who rightfully hold them.

Notwithstanding the foregoing, third party software (including open source software) used by ISRG to provide its services is licensed, not owned, by ISRG.

9.6 Representations and warranties

9.6.1 CA representations and warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, ISRG does not make any representations or warranties regarding its products or services. ISRG represents and warrants, to the extent specified in this CPS, that:

1. ISRG complies, in all material aspects, with the CP and this CPS,
2. ISRG publishes and updates CRLs and OCSP responses on a regular basis,
3. All certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the CAB Forum Baseline Requirements, and
4. ISRG will maintain a repository of public information on its website.

9.6.2 RA representations and warranties

Each RA represents and warrants that:

1. The RA's certificate issuance and management services conform to the ISRG CP and this CPS,
2. Information provided by the RA does not contain any false or misleading

information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All certificates requested by the RA meet the requirements of this CPS.

ISRG's agreement with the RA may contain additional representations and warranties.

9.6.3 Subscriber representations and warranties

1. Each Subscriber warrants to ISRG and the public-at-large that Subscriber is the legitimate registrant of the Internet domain name that is, or is going to be, the subject of the ISRG certificate issued to Subscriber, or that Subscriber is the duly authorized agent of such registrant.
2. Each Subscriber warrants to ISRG and the public-at-large that either (a) Subscriber did not obtain control of such domain name as the result of a seizure of such domain name, or (b) such domain name had no ongoing lawful uses at the time of such seizure.
3. Each Subscriber warrants that all information in the ISRG certificate issued to Subscriber regarding Subscriber or its domain name is accurate, current, reliable, complete, and not misleading.
4. Each Subscriber warrants that all information provided by Subscriber to ISRG is accurate, current, complete, reliable, complete, and not misleading.
5. Each Subscriber warrants that Subscriber rightfully holds the Private Key corresponding to the Public Key listed in the ISRG certificate issued to Subscriber.
6. Each Subscriber warrants that Subscriber has taken all appropriate, reasonable, and necessary steps to secure and keep Subscriber's Private Key secret.
7. Each Subscriber acknowledges and accepts that ISRG is entitled to revoke Subscriber's ISRG certificates immediately if the Subscriber violates the terms of the Subscriber Agreement or if ISRG discovers that any of Subscriber's ISRG certificates are being used to enable criminal activities

such as phishing attacks, fraud, or the distribution of malware.

9.6.4 Relying party representations and warranties

Each Relying Party represents and warrants that, prior to relying on an ISRG certificate, it:

1. Obtained sufficient knowledge on the use of digital certificates and PKI,
2. Studied the applicable limitations on the usage of certificates and agrees to ISRG's limitations on its liability related to the use of certificates,
3. Has read, understands, and agrees to this CPS,
4. Verified both the ISRG certificate and the certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use an ISRG certificate if the certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on an ISRG certificate after considering:
    - Applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    - The intended use of the certificate as listed in the certificate or this CPS,
    - The data listed in the certificate,
    - The economic value of the transaction or communication,
    - The potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    - The Relying Party's previous course of dealing with the Subscriber,
    - The Relying Party's understanding of trade, including experience with computer-based methods of trade, and
    - Any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a certificate is at a party's own risk.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

ISRG CERTIFICATES AND SERVICES ARE PROVIDED “AS-IS.” ISRG DISCLAIMS ANY AND ALL WARRANTIES OF ANY TYPE, WHETHER EXPRESS OR IMPLIED, INCLUDING AND WITHOUT LIMITATION ANY IMPLIED WARRANTY OF TITLE, NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE, IN CONNECTION WITH ANY ISRG SERVICE OR ISRG CERTIFICATE.

9.8 Limitations of liability

ISRG DOES NOT ACCEPT ANY LIABILITY FOR ANY LOSS, HARM, CLAIM, OR ATTORNEY’S FEES IN CONNECTION WITH ANY CERTIFICATES. ISRG WILL NOT BE LIABLE FOR ANY DAMAGES, ATTORNEY’S FEES, OR RECOVERY, REGARDLESS OF WHETHER SUCH DAMAGES ARE DIRECT, CONSEQUENTIAL, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR COMPENSATORY, EVEN IF ISRG HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION ON LIABILITY APPLIES IRRESPECTIVE OF THE THEORY OF LIABILITY, I.E., WHETHER THE THEORY OF LIABILITY IS BASED UPON CONTRACT, WARRANTY, INDEMNIFICATION, CONTRIBUTION, TORT, EQUITY, STATUTE OR REGULATION, COMMON LAW, OR ANY OTHER SOURCE OF LAW, STANDARD OF CARE, CATEGORY OF CLAIM, NOTION OF FAULT OR RESPONSIBILITY, OR THEORY OF RECOVERY. THIS DISCLAIMER IS INTENDED TO BE CONSTRUED TO THE FULLEST EXTENT ALLOWED BY APPLICABLE LAW.

WITHOUT WAIVING OR LIMITING THE FOREGOING IN ANY WAY, ISRG DOES NOT MAKE, AND ISRG EXPRESSLY DISCLAIMS, ANY WARRANTY REGARDING ITS RIGHT TO USE ANY TECHNOLOGY, INVENTION, TECHNICAL DESIGN, PROCESS, OR BUSINESS METHOD USED IN EITHER ISSUING CERTIFICATES OR

PROVIDING ANY OF ISRG'S SERVICES. EACH SUBSCRIBER AFFIRMATIVELY AND EXPRESSLY WAIVES THE RIGHT TO HOLD ISRG RESPONSIBLE IN ANY WAY, OR SEEK INDEMNIFICATION AGAINST ISRG, FOR ANY INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS, INCLUDING PATENT, TRADEMARK, TRADE SECRET, OR COPYRIGHT.

9.9 Indemnities

9.9.1 Indemnification by ISRG

The CA does not provide any indemnification except as described in Section 9.9.1 of the Certificate Policy.

9.9.2 Indemnification by Subscribers

Each Subscriber will indemnify and hold harmless ISRG and its directors, officers, employees, agents, and affiliates from any and all liabilities, claims, demands, damages, losses, costs, and expenses, including attorneys' fees, arising out of or related to: (i) any misrepresentation or omission of material fact by Subscriber to ISRG, irrespective of whether such misrepresentation or omission was intentional, (ii) Subscriber's violation of the Subscriber Agreement, (iii) any compromise or unauthorized use of an ISRG certificate or corresponding Private Key, or (iv) Subscriber's misuse of an ISRG certificate. If applicable law prohibits Subscriber from providing indemnification for another party's negligence or acts, such restriction, or any other restriction required by law for this indemnification provision to be enforceable, shall be deemed to be part of this indemnification provision.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify ISRG, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of any

service terms applicable to the services provided by ISRG or its affiliates and used by the Relying Party, this CPS, or applicable law; (ii) unreasonable reliance on a certificate; or (iii) failure to check the certificate's status prior to use.

9.10 Term and termination

9.10.1 Term

This CPS and any amendments to this CPS are effective when published to the ISRG online repository and remain in effect until replaced with a newer version.

9.10.2 Termination

This CPS and any amendments remain in effect until replaced with a newer version.

9.10.3 Effect of termination and survival

ISRG will communicate the conditions and effect of this CPS's termination via the ISRG Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the certificate is revoked or expired, even if this CPS terminates.

9.11 Individual notices and communications with participants

ISRG accepts notices related to this CPS at the locations specified in Section 1.5.2 of this CPS. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from ISRG. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 1.5.2 of this CPS using either a courier service that confirms delivery or via certified or registered mail with postage

prepaid and return receipt requested. ISRG may allow other forms of notice in its Subscriber Agreements.

9.12 Amendments

9.12.1 Procedure for amendment

This CPS is reviewed at least annually and may be reviewed more frequently. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place that are designed to reasonably ensure that this CPS is not amended and published without the prior authorization of the ISRG PMA.

9.12.2 Notification mechanism and period

ISRG posts CPS revisions to its Repository. ISRG does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice.

9.12.3 Circumstances under which OID must be changed

The ISRG PMA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13 Dispute resolution provisions

Any claim, suit or proceeding arising out of this CPS or any ISRG product or service must be brought in a state or federal court located in San Jose, California. ISRG may seek injunctive or other relief in any state, federal, or national court of competent jurisdiction for any actual or alleged infringement of its, its affiliates, or any third party's intellectual property or other proprietary rights.

9.14 Governing law

The laws of the state of California, United States of America, govern the interpretation, construction, and enforcement of this CPS and all proceedings related to ISRG products and services, including tort claims, without regard to any conflicts of law principles. The United Nations Convention for the International Sale of Goods does not apply to this CPS.

9.15 Compliance with applicable law

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

ISRG contractually obligates each RA to comply with this CPS and applicable industry guidelines. ISRG also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2 Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of ISRG. Unless specified otherwise in a contract with a party, ISRG does not provide notice of assignment.

9.16.3 Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

ISRG may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. ISRG's failure to enforce a provision of this CPS does not waive ISRG's right to enforce the same provision later or right to enforce any other provision of this CPS. To be effective, waivers must be in writing and signed by ISRG.

9.16.5 Force Majeure

ISRG is not liable for any delay or failure to perform an obligation under this CPS to the extent that the delay or failure is caused by an occurrence beyond ISRG's reasonable control. The operation of the Internet is beyond ISRG's reasonable control.

9.17 Other provisions

No stipulation.

EXHIBIT C

From: **Benjamin Costa** ben@rcjlawgroup.com
Subject: Fwd: Demand for Cancellation of Domain Name- herbalalchemist.com
Date: June 9, 2017 at 10:38 AM
To: klundy@phillipsnizer.com
Cc: monicam@phillipsnizer.com, Chris K. Ridder chris@rcjlawgroup.com
Bcc: Benjamin A. Costa ben@rcjlawgroup.com

Dear Ms. Lundy,

This firm represents ISRG. Further to the below, we have reviewed your request concerning the herbal-alchemist.com domain name. As our client has informed you, Let's Encrypt security certificates are offered on a free, automated, and open basis to internet users throughout the world. These security certificates are designed only to provide privacy and data integrity between two communicating computer systems, and play no part in any infringing activity occurring on or through the herbal-alchemist.com domain name. Disabling the SSL certificate would not affect the content or availability of the site or its domain name.

Our client's potential liability for such services is set forth in *Perfect 10, Inc. v. Visa Int'l Serv. Ass'n*, 494 F.3d 788 (9th Cir. 2007) (no liability). In addition, the order you sent does not apply to ISRG, which is not acting in concert or participation with herbal-alchemist.com. ISRG's security certificates simply have no nexus to any infringement that may be occurring on or through the site you've brought to our attention.

We suggest you contact the relevant web/domain hosts, to request that the website and/or domain name be disabled. However, if you'd like to discuss this matter further, we can make ourselves available for a call next week for that purpose.

Yours truly,
-Ben

Benjamin A. Costa
Ridder, Costa & Johnstone LLP
12 Geary St., Ste 701
San Francisco, CA 94108
Email: ben@rcjlawgroup.com
GPG Key (2015-): https://goo.gl/1cjbDf
Tel: (415) 391-3311
Fax: (415) 358-4975

---------- Forwarded message ----------
From: "Kathryn T. Lundy" <klundy@phillipsnizer.com>
Date: Jun 7, 2017 1:08 PM
Subject: Demand for Cancellation of Domain Name- herbalalchemist.com
To: "josh@letsencrypt.org" <josh@letsencrypt.org>
Cc: "Monica P. McCabe" <monicam@phillipsnizer.com>

> Mr. Aas:
>
> Further to your e-mail below, please forward to legal counsel Herbalist & Alchemist, Inc.'s Demand for Cancellation of Domain Name -herbalalchemist.com, along with the referenced March 8, 2017 Court Order directing the same, as we intend to pursue the matter further with the Court if there is no resolution of this issue by Let's Encrypt.
>
> I look forward to a prompt response from legal counsel. Thank you for your attention to this matter.
>
> Kathryn T. Lundy, Esq.
> ***PHILLIPS NIZER LLP***

666 Fifth Avenue

New York, New York 10103-0084
Direct: (212) 841-0544

E-mail: klundy@phillipsnizer.com

www.phillipsnizer.com

From: Josh Aas [mailto:josh@letsencrypt.org]
Sent: Thursday, June 01, 2017 2:04 PM
To: Kathryn T. Lundy
Cc: Monica P. McCabe
Subject: Re: Demand for Cancellation of Domain Name- herbalalchemist.com

Dear Ms. McCabe,

Thank you for your note. Unfortunately, the Internet Security Research Group ("ISRG") is not in a position to adjudicate trademark disputes, and so must deny your request that the security certificate in question be revoked.

ISRG provides Let's Encrypt security certificates on a free, automated, and open basis to internet users throughout the world. These security certificates are designed only to provide privacy and data integrity between two communicating computer applications. We have no control over the domain name referenced in your request, or any material made available at that domain. We have no relationship with the party or parties who own and/or control the domain name at all, except that they appear to be users of Let's Encrypt security certificate service. We do not host content for any third-party user of the Let's Encrypt service.

Though we are sympathetic to brand owners who feel their marks may be being infringed, we encourage you to address any future concerns you may have regarding the domain name, or any content appearing at the domain, to the registrant and/or owner of the domain name itself, or to the website's hosting provider. That said, we would of course be happy to forward your request to our legal counsel so that you can discuss it in more detail with them directly, if you would prefer.

--
Josh Aas
Executive Director
Internet Security Research Group
Let's Encrypt: A Free, Automated, and Open CA

On Thu, May 25, 2017 at 2:31 PM, Kathryn T. Lundy
<klundy@phillipsnizer.com> wrote:
> Legal Department:
>
> On behalf of Herbalist & Alchemist, Inc., attached please find a Demand for
> Cancellation of Domain Name -herbalalchemist.com, along with the referenced
> March 8, 2017 Court Order directing the same.
>
> Regards,
>
> Kathryn T. Lundy, Esq.
> PHILLIPS NIZER LLP

>
> 666 Fifth Avenue
>
> New York, New York 10103-0084
> Direct: (212) 841-0544
>
> E-mail: klundy@phillipsnizer.com
>
> www.phillipsnizer.com

PHILLIPS NIZER LLP

666 Fifth Avenue
New York, NY 10103-0084
212.977.9700
Fax 212.262.5152

600 Old Country Road
Garden City, NY 11530-2011
516.229.9400
Fax 516.228.9612

Court Plaza South
21 Main Street
Hackensack, NJ 07601
201.487.3700
Fax 201.646.1764

www.phillipsnizer.com

Monica Petraglia McCabe
212.841.0713
mmccabe@phillipsnizer.com

May 25, 2017

Via Regular Mail and Electronic Mail – press@letsencrypt.org

Let's Encrypt
1 Letterman Drive, Suite D4700
San Francisco, CA 94129
c/o Legal Department

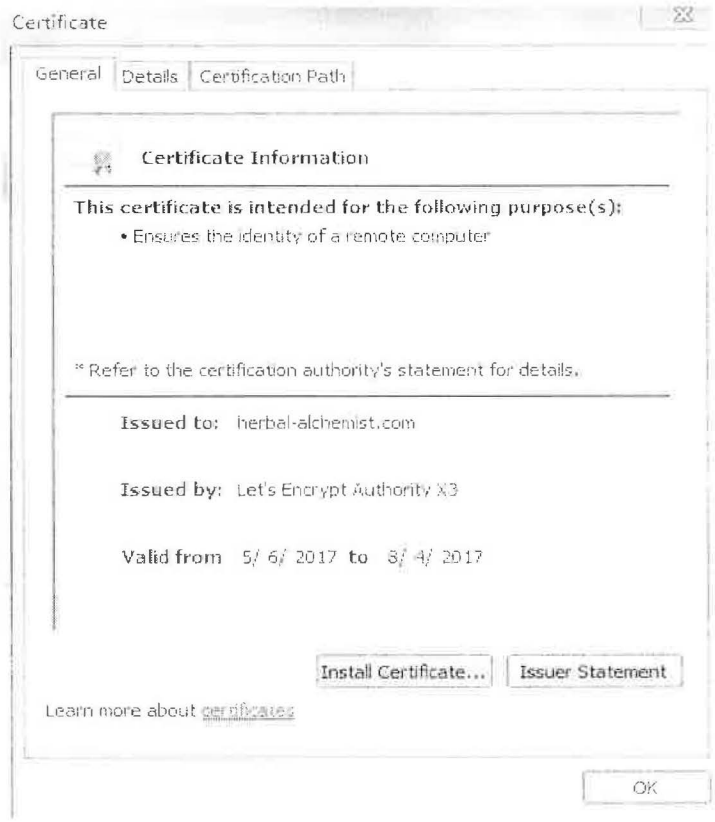
Re: Demand for Cancellation of SSL Certificates - https://herbal-alchemist.com/

Dear Legal Department:

This firm represents Herbalist & Alchemist, Inc. ("Herbalist & Alchemist") in connection with the above referenced matter and we are authorized to act on its behalf as owner of certain intellectual property rights.

This letter serves to provide notice of trademark infringement relating to the mark HERBALIST & ALCHEMIST not authorized for use by the above named domain name owner or agents.

Specifically, Alurent Products, Inc. ("Alurent") has been and is now distributing dietary and nutritional supplements as well as other herbal and botanical products under the name "herbalalchemist," which is referenced and promoted on the website herbal-alchemist.com, a domain hosted by OVH Hosting, Inc. operating with a Certificate issued by Let's Encrypt, as show in below image. Such use is a violation of Herbalist & Alchemist's rights under United States federal and state law.



Given Alurent's unlawful use and infringment of Herbalist & Alchemist's trademark, Herbalist & Alchemist filed a federal district court lawsuit in the United Stated District Court, Southern District Court of New York ("Court") identified as *Herbalist & Alchemist, Inc. v. Alurent Products, Inc. and Will Clarent*, and bearing civil action no: 16-cv-09204-ER.

On March 8, 2017, the Court entered an Order ("March 8, 2017 Order") against Alurent and its principal, granting judgment and permanent injunctions against them. The Order provides, in relevant part, as follows:

- Alurent is liable to Herbalist & Alchemist for violation of 15 U.S.C. § 1125(a) in that they have used in connection with their goods false designations of origin and false descriptions or representations tending to falsely describe or represent the same.

- Alurent is liable to Herbalist & Alchemist for violation of 15 U.S.C. § 1125(a)(1)(B) for false, deceptive and misleading descriptions and misrepresentations in commercial advertising, labeling and marketing, which

misrepresent the nature, characteristics and qualities of its products in interstate commerce.

- Alurent is liable to Herbalist & Alchemist for violation of 15 U.S.C. § 1125(a)(1)(A) for unfair competition and passing off.

- Alurent is liable to Herbalist & Alchemist for violation of 15 U.S.C. § 1125(d)(1)(A) for bad faith cyberpiracy.

- Alurent is liable to Herbalist & Alchemist for violation of New York Common Law Unfair Competition.

- Alurent is liable to Herbalist & Alchemist for violation of Section 349(a) and (h) and 350 and 350-a of the New York General Business Law.

- **Alurent, its directors, principals, officers, agents, representatives, servants, employees, attorneys, successors and assigns, and all others in active concert or participation with them, are permanently enjoined and restrained from**:

(a) **imitating, copying, or making any other infringing use or providing services bearing Plaintiff's mark, HERBALIST & ALCHEMIST** (the **"Mark"**);

(b) providing, producing, distributing, offering for distribution, circulating, selling, offering for sale, **advertising**, importing, **promoting**, or **displaying any services bearing any simulation, reproduction, counterfeit, copy, or colorable imitation of the Mark**;

(c) using any simulation, reproduction, counterfeit, copy, or colorable imitation of the Mark in connection with the provision, distribution, offering for distribution, circulation, sale, offering for sale, import, advertisement, promotion, or display of any services not authorized or licensed by Herbalist & Alchemist;

(d) **using any false designation of origin or false description which can or is likely to lead the trade or public or individuals erroneously to believe that services have been provided, offered, circulated, sold, offered for sale, advertised, promoted, displayed, licensed, sponsored, approved, or authorized by or for Herbalist & Alchemist, when such is not true in fact**;

(e) publishing, displaying, distributing or using, permitting or entering into or performing any agreement for the publication, display, distribution or use of false, deceptive or misleading advertisement and labeling of its products;

(f) engaging in any other activity constituting an infringement of the Mark, or of Herbalist & Alchemist's right in, or right to use or to exploit its Mark; and

(g) assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activities referred to in subparagraphs (a) through (f) above.

In addition, the Court also ordered and directed that:

- Alurent bear the obligation and expense of publication, display distribution and dissemination of corrective advertising to dispel the false, misleading and deceptive advertising already communicated to the public and Herbalist & Alchemist's customers;

- the destruction of all labels, signs, prints, packages receptacles, advertisements and promotions in the possession of Alurent bearing the name that is the subject of the aforementioned claims under 15 U.S.C. § 1118;

- **the Commissioner of Trademarks, pursuant to 15 U.S.C. § 1119, to either order Alurent to abandon the herbalalchemist application within thirty days of this Order or deny Alurent's Application to register the herbalalchemist mark (Serial No. 86854880);**

- **the Commissioner of Trademarks, pursuant to 15 U.S.C. § 1119 to grant Herbalist & Alchemist, Inc.'s application to register the HERBALIST & ALCHEMIST Mark (Serial No. 87042871); and**

- **the forfeiture to Plaintiff or cancellation of the domain name "herbal-alchemist".**

A copy of the March 8, 2017 Order is attached hereto at Exhibit "A."

Given the Court's March 8, 2017 Order, we hereby request that you act expeditiously to revoke the SSL Certificates issued to the website host platform OVH Hosting, Inc. which hosts https://herbal-alchemist.com/. Herbal Alchemist is operating the website for which the Certificate was issued in violation of the March 8, 2017 Order.

To protect my client's rights and interest for trademark infringement and misappropriation, please ensure the referenced SSL Certificates are cancelled from your platform within five (5) days.

This letter is written without prejudice to any of my client's rights or remedies available under the law, which are expressly reserved herein. Please contact me should you have any questions.

Very truly yours,

Monica P. McCabe

Attachment

EXHIBIT A

[to the document sent by counsel for Plaintiff as an attachment to their email of May 25, 2017]

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

HERBALIST & ALCHEMIST, INC.

Plaintiff,

- against -

ALURENT PRODUCTS, INC. and WILL CLARENT,

Defendants..

DEFAULT JUDGMENT AGAINST DEFENDANTS ALURENT PRODUCTS, INC. and WILL CLARENT

16 Civ. 09204 (ER)

Having considered Plaintiff Herbalist & Alchemist, Inc.'s ("Plaintiff") Application for Entry of Default Judgment and Permanent Injunction, the Memorandum of Law in Support thereof, the Affidavit of Elizabeth Lambert, the Declaration of Monica P. McCabe, Esq., in support thereof, the Summons, the Complaint, and proofs of service on file herein, and all of the relevant papers and pleadings on file with the Court in this matter,

THE COURT ORDERS AND DETERMINES AS FOLLOWS:

1. Plaintiff's Application for Default Judgment and Permanent Injunction Against Defendants Alurent Products, Inc. and Will Clarent ("Defendants") is GRANTED;

2. Defendants are liable to Plaintiff for violation of 15 U.S.C. § 1125(a) in that Defendants have used in connection with their goods false designations of origin and false descriptions or representations tending to falsely describe or represent the same.

3. Defendants are liable to Plaintiff for violation of 15 U.S.C. § 1125(a)(1)(B) for false, deceptive and misleading descriptions and misrepresentations in commercial advertising,

labeling and marketing, which misrepresent the nature, characteristics and qualities of its products in interstate commerce.

4. Defendants are liable to Plaintiff for violation of 15 U.S.C. § 1125(a)(1)(A) for unfair competition and passing off.

5. Defendants are liable to Plaintiff for violation of 15 U.S.C. § 1125(d)(1)(A) for bad faith cyberpiracy.

6. Defendants are liable to Plaintiff for violation of New York Common Law Unfair Competition.

7. Defendants are liable to Plaintiff for violation of Section 349(a) and (h) and 350 and 350-a of the New York General Business Law.

8. Plaintiff is entitled to recover statutory damages in this action pursuant to 15 U.S.C. § 1117(c), in the amount of $50,000.00 as against each Defendant.

9. Plaintiff is entitled to recover its reasonable attorneys' fees incurred in this action pursuant to 15 U.S.C. § 1117(a), and has sufficiently substantiated the amount of reasonable attorneys' fees in the amount of $45,403.00;

10. Plaintiff is entitled to recover its costs of the action in the amount of $1,410.44; and

11. Plaintiff is hereby awarded judgment against Defendants, jointly and severally, as follows:

a. Statutory Damages.....$50,000.00

b. Attorneys' Fees.....$45,403.00

c. Costs.....$1,410.44

Total Judgment $96,813.44

This judgment shall accrue interest, compounded annually, pursuant to 28 U.S.C. § 1961.

In addition, Defendants, their directors, principals, officers, agents, representatives, servants, employees, attorneys, successors and assigns, and all others in active concert or participation with Defendants, be permanently enjoined and restrained from:

(a) imitating, copying, or making any other infringing use or providing services bearing Plaintiff's mark, HERBALIST & ALCHEMIST (the "Mark");

(b) providing, producing, distributing, offering for distribution, circulating, selling, offering for sale, advertising, importing, promoting, or displaying any services bearing any simulation, reproduction, counterfeit, copy, or colorable imitation of Plaintiff's Mark;

(c) using any simulation, reproduction, counterfeit, copy, or colorable imitation of Plaintiff's Mark in connection with the provision, distribution, offering for distribution, circulation, sale, offering for sale, import, advertisement, promotion, or display of any services not authorized or licensed by Plaintiff;

(d) using any false designation of origin or false description which can or is likely to lead the trade or public or individuals erroneously to believe that services have been provided, offered, circulated, sold, offered for sale, advertised, promoted, displayed, licensed, sponsored, approved, or authorized by or for Plaintiff, when such is not true in fact;

(e) publishing, displaying, distributing or using, permitting or entering into or performing any agreement for the publication, display, distribution or use of false, deceptive or misleading advertisement and labeling of its products;

(f) engaging in any other activity constituting an infringement of Plaintiff's Mark, or of Plaintiff's right in, or right to use or to exploit its Mark; and

(g) assisting, aiding, or abetting any other person or business entity in engaging in or performing any of the activities referred to in subparagraphs (a) through (f) above.

In addition, the Court further orders and directs that:

(a) Defendants bear the obligation and expense of publication, display distribution and dissemination of corrective advertising to dispel the false, misleading and deceptive advertising already communicated to the public and Plaintiff's customers.

(b) the destruction of all labels, signs, prints, packages receptacles, advertisements and promotions in the possession of Defendants bearing the name that is the subject of the aforementioned claims under 15 U.S.C. § 1118;

(c) the Commissioner of Trademarks, pursuant to 15 U.S.C. § 1119, to either order Defendants to abandon the herbalalchemist application within thirty days of this Order or deny Defendants' Application to register the herbalalchemist mark (Serial No. 86854880).

(d) the Commissioner of Trademarks, pursuant to 15 U.S.C. § 1119 to grant Plaintiff's application to register the HERBALIST & ALCHEMIST Mark (Serial No. 87042871); and

(e) the forfeiture to Plaintiff or cancellation of the domain name "herbal-alchemist".

IT IS SO ORDERED AND ADJUDGED.

DATED: March 8, 2017
New York, New York

Edgardo Ramos, U.S.D.J.

EXHIBIT D

crt.sh Certificate Search

Criteria	ID = '133673877'

crt.sh ID	133673877
Summary	Leaf certificate
Certificate Transparency	

Timestamp	Entry #	Log Operator	Log URL
2017-05-06 15:00:29 UTC	55718961	Google	https://ct.googleapis.com/icarus
2017-05-06 15:00:29 UTC	14675847	Venafi	https://ctlog-gen2.api.venafi.com
2017-05-08 20:01:29 UTC	100558864	Google	https://ct.googleapis.com/pilot
2017-05-08 21:24:42 UTC	97509150	Google	https://ct.googleapis.com/rocketeer

Revocation

Mechanism	Provider	Status	Revocation Date	Last Observed in CRL	Last Checked (Error)
CRL	The CA	Unknown	n/a	n/a	
CRLSet/Blacklist	Google	Not Revoked	n/a	n/a	n/a
disallowedcert.stl	Microsoft	Not Revoked	n/a	n/a	n/a
OneCRL	Mozilla	Not Revoked	n/a	n/a	n/a

SHA-256(Certificate)	2DA05E68467A2E7AC679357548DF0E47D15185D50EA1B4F47F604E4666B05392
SHA-1(Certificate)	FF2075720794CB921F6C17FF49B29D265AC354A2

Certificate | ASN.1

Hide metadata

Run cablint

Run x509lint

Download Certificate: PEM

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            03:b6:03:35:75:ba:df:5a:c7:d3:9e:a3:09:5e:2a:85:87:6c
    Signature Algorithm: sha256WithRSAEncryption
        Issuer:
            commonName                = Let's Encrypt Authority X3
            organizationName          = Let's Encrypt
            countryName               = US
        Validity
            Not Before: May  6 14:00:00 2017 GMT
            Not After : Aug  4 14:00:00 2017 GMT
        Subject:
            commonName                = herbal-alchemist.com
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:b9:f1:7f:91:d5:22:67:51:cd:4b:b3:95:d0:ce:
                    55:f9:93:19:99:93:68:4d:55:24:52:d6:d1:0b:c2:
                    4b:23:f3:15:a2:ce:df:6a:dc:71:3f:2a:be:96:94:
                    ef:96:af:b7:12:21:98:e1:c3:5e:26:30:0b:2e:db:
                    7a:94:bd:a3:cf:da:f0:b8:40:58:53:04:cb:e8:ea:
                    d8:8c:f1:87:7f:d6:a8:01:49:a6:4e:90:a6:c8:f2:
                    d8:ff:db:70:0f:1e:18:4f:3c:5c:97:e0:42:03:8d:
                    64:84:27:e4:68:74:cc:b3:9b:2c:0c:42:5b:4b:b7:
                    c0:78:54:b3:0d:20:21:0d:9b:aa:40:aa:59:24:80:
                    ff:e0:6b:f6:70:87:10:2f:69:75:b4:41:41:f3:bf:
                    ef:4f:92:0b:96:91:c0:f9:a5:e2:4c:dc:14:3a:af:
                    d5:d4:e4:b2:e5:6a:88:8b:6f:56:86:ca:fa:fb:d5:
                    89:1e:c0:49:a7:d7:bc:ac:aa:a3:e3:56:5c:13:22:
                    96:ba:61:be:3b:c2:56:97:21:9d:f2:26:1c:5a:88:
                    cd:76:67:ef:e3:cf:77:8b:0e:a3:6f:d2:7e:39:fa:
                    5b:98:02:86:0f:86:9d:6b:6f:9a:62:9c:d3:cb:2d:
                    50:b2:7c:9f:1e:95:1b:3a:15:df:7f:03:e0:49:f1:
                    c2:3f
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Key Usage: critical
                Digital Signature, Key Encipherment
            X509v3 Extended Key Usage:
                TLS Web Server Authentication, TLS Web Client Authentication
            X509v3 Basic Constraints: critical
                CA:FALSE
            X509v3 Subject Key Identifier:
                1F:5E:D7:E0:23:22:AF:3E:D4:52:8B:4D:F3:63:37:10:96:F2:12:2F
            X509v3 Authority Key Identifier:
                keyid:A8:4A:6A:63:04:7D:DD:BA:E6:D1:39:B7:A6:45:65:EF:F3:A8:EC:A1

            Authority Information Access:
                OCSP - URI:http://ocsp.int-x3.letsencrypt.org/
                CA Issuers - URI:http://cert.int-x3.letsencrypt.org/

            X509v3 Subject Alternative Name:
                DNS:herbal-alchemist.com
                DNS:www.herbal-alchemist.com
            X509v3 Certificate Policies:
                Policy: 2.23.140.1.2.1
                Policy: 1.3.6.1.4.1.44947.1.1.1
                  CPS: http://cps.letsencrypt.org
                  User Notice:
                    Explicit Text: This Certificate may only be relied upon by Relying Parties and only in accordance with the Certificate Policy found a

    Signature Algorithm: sha256WithRSAEncryption
         1b:07:bb:e5:71:73:1a:27:fa:6e:34:09:c7:64:19:c9:2a:19:
         68:8f:bd:e1:06:6e:51:36:1f:f2:a5:6b:17:85:0d:a7:0e:39:
         78:45:ed:45:22:d1:7d:37:85:b1:73:fc:15:8f:b4:e6:04:41:
         65:69:77:82:34:f2:73:bf:cf:13:09:9a:1b:85:e0:f5:be:9b:
         10:1d:95:3a:7c:2b:47:36:34:75:17:5b:4d:31:90:28:8f:86:
         c7:00:d8:1b:50:01:e7:9e:d1:b0:80:a6:56:9c:fb:da:29:b3:
         d3:47:cb:b9:8b:b4:2a:8a:ff:2c:76:ba:90:cb:f4:c5:53:14:
         75:77:a2:70:ce:76:59:de:8a:95:16:91:df:77:5a:87:ad:d6:
         99:73:61:23:1b:3b:82:14:bf:bb:f2:cd:f7:84:18:e2:87:64:
         82:bf:df:c2:20:19:41:8d:03:66:f2:b5:77:be:6c:3a:97:88:
         38:6e:5c:5f:36:09:7c:ad:fd:71:36:a7:be:a6:bd:9a:91:fc:
         40:90:6c:4e:73:18:9c:c3:9c:7e:e1:44:97:20:7c:49:80:fc:
         59:cb:87:2e:9e:cb:af:e2:9f:5b:1b:43:66:06:b0:ac:a1:cb:
         76:6c:a7:2c:f4:6d:94:cf:5a:73:f2:8e:05:97:72:79:34:91:
         52:79:64:0f
```